St Ambrose Catholic Primary School
Remote Education Policy

Date of Ratification:		Signed: Mrs E. Brocklesby (Principal) Mrs J.Rowe (Acting Chair Of Academy Committee)
Review date:		Signed: Mrs E. Brocklesby (Principal) Mrs J. Rowe (Acting Chair Of Academy Committee)

Remote Education Policy for St. Ambrose Catholic Primary School

1. Statement of School's Curriculum Aims

St. Ambrose Catholic Primary School aims to deliver a curriculum which is relevant for our pupils and the community in which they live. We have aimed to create an ambitious and engaging curriculum which engages pupils and therefore has a positive impact on learning.

2. Aims

This Remote Education Policy aims to:

- Ensure consistency in the approach to remote learning for all pupils (Inc. SEND) who aren't in school, through use of quality online and offline resources and teaching videos
- Provide clear expectations to members of the school community with regards to delivering high quality, interactive remote learning
- Include continuous delivery of the school curriculum aims, as far as possible, as well as support of pupils' social and emotional wellbeing
- Consider continued education for staff and parents (e.g. CPD, Parents Workshops and Meet the Teacher)
- Support effective communication between the school and families and support attendance

3. Who is this policy applicable to?

- A child *(and their siblings if they are also attending St. Ambrose Catholic Primary School)* is absent because they are awaiting test results and the household is required to self-isolate. The rest of their school bubble are attending school and being taught as normal.
- A child's whole bubble is not permitted to attend school because they, or another member of their bubble, have tested positive for Covid-19.

Remote learning will be shared via Purple Mash or Teams when pupils are absent due to Covid-related reasons and not necessarily to all at the start of week, unless the class teacher deems this appropriate.

4. Content and Tools to Deliver This Remote Education Plan

Resources to deliver this Remote Education Plan include:

- Online tools for EYFS, KS1 & KS2 *(Purple Mash [including Mini Mash and Serial Mash])* and Teams when appropriate (also used for staff CPD and parent/carer sessions*).*
- Phone calls home (where staff are present on site)
- Printed learning packs (where necessary)
- Physical materials such as story books and writing tools (where available)

Use of BBC Teach, BBC Bitesize, Oak Academy, Maths Shed ,Spelling Shed, Oxford Owl, and Education City

- The following timetables can be found in the appendix:
  - Model Timetable and structure for remote learning in the event of whole-bubble closure. This will be adapted by teachers at the beginning of each week and will be as close as possible to the normal timetable in school. (Appendix 1)
  - Model timetable and structure for remote learning in the event of a small number of pupils self-isolating. This is a suggested structure for parents/carers to follow if their child(ren) are well enough to attempt school work at home. (Appendix 2)

    Each day, work for each lesson will be set on Purple Mash or set by teacher on Teams. Some lessons will be completed online, whilst others will encourage children to complete an activity away from the screen.

Remote learning should be carried out in line with the following:

- Teacher and Pupil Code of Conduct for Phone calls, Video calls and Recorded Video (Appendix 3)

5. Home and School Partnership

St. Ambrose Catholic Primary School is committed to working in close partnership with families and recognises each family is unique and because of this, remote learning will look different for different families in order to suit their individual needs.

St. Ambrose Catholic Primary School has provided training for staff on use of Purple Mash. Staff will also provide pupils with a refresher session on how to use Purple Mash and where to find and upload work.
Where possible, it is beneficial for young people to maintain a regular and familiar routine. St. Ambrose Catholic Primary School would recommend that each 'school day' maintains structure

We would encourage parents to support their children's work, including finding an appropriate place to work and, to the best of their ability, support pupils with work encouraging them to work with good levels of concentration.

Every effort will be made by staff to ensure that work is set promptly. Should accessing work be an issue, parents/carers should contact the class teacher promptly and alternative solutions may be available. These will be discussed on a case-to-case basis.

We would encourage parents/carers to familiarise themselves with St. Ambrose Catholic Primary School's e-safety policy and the e-safety resources in the COVID-19 tab on the school website, to support a healthy and balanced digital diet for pupils.

All children are expected to follow the same e-safety rules they would at school.

6. Roles and responsibilities

Teachers

To note: the suggested responsibilities below relate to where a whole class/bubble is isolating and would be reduced when it is fewer children isolating and the majority of the class are in school.

When providing remote learning, teachers must be available during their normal working hours.

If they are unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure.

When providing remote learning, teachers are responsible for:

- Registration of pupils via Purple Mash:
- In the event of a whole-bubble, or whole-school closure, teachers will email a record of attendance to admin staff daily by 9:30am
- Setting work:
- Teachers will set differentiated work for the pupils in their classes daily
- Teachers will include instructions on when and how to submit work
- The work set should follow the usual timetable for the class had they been in school, wherever possible
- Teachers will set work on Purple Mash and select objectives relevant to the learning
- Where only part of the bubble is self-isolating, teachers will upload work to Purple Mash that has been taught in class during the day. This will be done as soon as practically possible, but no later than the end of the same working day. In this case, pupils will complete the work the following day
- Providing feedback on work:

All work will be responded to as soon as practically possible by teachers or teaching assistants, but will be guided by the following:

- Reading, writing and maths work submitted during the lesson time will be responded to, by adults, during the lesson time. Any work submitted outside lesson time, but by 1pm, will be responded to, by 4pm, wherever practically possible.
- All curriculum tasks submitted by 3.30pm will be responded to where ever practically possible before the next lesson due.
- Pupils and adults may have an ongoing dialogue via Purple Mash emails, during lesson time, in which support and feedback will be provided.
- Adults will provide feedback for pupils in the comments box on Purple Mash for each piece of work and assess against the objectives set, where ever practically possible.
- Where only part of the bubble is self-isolating, adults will provide feedback to work, which has been submitted by 3pm, by 8:30am of the next school day where ever practically possible.
- Keeping in touch with pupils who aren't in school and their parents:
- If there is a concern around the level of engagement of a pupil(s) at the end of the second day of absence, teachers will inform the Principal and Vice Principal, who will arrange for parents/carers to be contacted via phone to access whether school intervention can assist engagement.
- All parent/carer emails should come through the school admin account (office@st-ambrose.worcs.sch.uk) or directly to class email addresses (details sent via email, please contact the school office if a copy if needed).
- Any complaints or concerns shared by parents or pupils should be reported to a member of SLT– for any safeguarding concerns, refer immediately to the DSL
- Following the code of conduct for remote learning and discussing with SLT if they feel they are unable to meet these requirements.

Teaching Assistants

Teaching assistants must be available during their normal working hours.

If they are unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure.

When supporting remote learning, teaching assistants are responsible for:

- Supporting pupils learning:
- Reply to emails through Purple Mash to support children's learning during allocated subject time
- Take direction from the class teacher in relation to support required during a remote lesson
- Set intervention work daily on Purple Mash for a group of pupils
- Provide feedback through the comments box on Purple Mash to work set
- Following the code of conduct for remote learning and discussing with SLT if they feel they are unable to meet these requirements.

During the school day, teaching assistants may also be required to complete tasks set by a member of SLT

Senior Leaders

Alongside any teaching responsibilities, senior leaders are responsible for:

- Co-ordinating the remote learning approach across the school inc. daily monitoring of engagement.
- Monitoring the effectiveness of remote learning, through usual monitoring channels and processes and share this at Senior Leadership Team meetings and subsequent Staff Meetings.
- Share any adaptations to remote learning with parents/carers
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations

Designated safeguarding lead

The DSL is responsible for managing and dealing with all safeguarding concerns. For further information, please see the Safeguarding and Child Protection Policy.

IT Technician

IT technician is responsible for:

- Fixing issues with systems used to set and collect work
- Helping staff with any technical issues they're experiencing
- Reviewing the security of remote learning systems and flagging any data protection breaches to the data protection officer

The SENDCO

Liaising with the ICT technicians to ensure that the technology used for remote learning is accessible to all pupils and that reasonable adjustments are made where required.

- Ensuring that pupils with EHC plans continue to have their needs met while learning remotely, and liaising with the principal and other organisations to make any alternate arrangements for pupils with EHC plans
- Identifying the level of support
- Monitoring quality of work set for children with additional needs

The SBM

- Ensuring value for money when arranging the procurement of equipment or technology.
- Ensuring that the school has adequate insurance to cover all remote working arrangements.

School Admin (in the event of whole-school closure)

- Follow usual attendance procedures for any children not present in virtual lessons (as recorded by teachers) – see school attendance procedure COVID-19 addendum

Pupils and parents

Staff can expect pupils learning remotely to:

- Familiarise themselves with the Code of Conduct for video calls
- Log into Purple Mash at the beginning of the school day
- Check the timetable and work for each lesson throughout the day
- Complete work to the deadline set by teachers
- Seek help if they need it, from teachers or teaching assistants
- Alert teachers if they're not able to complete work

Staff can expect parents with children learning remotely to:

- Support children in understanding the Code of Conduct for video calls
- Make the school aware if their child is sick or otherwise can't complete work
- Seek help from the school if they need it
- Ensure pupils are supervised whilst at a computer or other device
- Familiarise themselves with e-safety guidelines
- Prioritise children's wellbeing and health
- Encourage child(ren) to do their best
- Be respectful when making any complaints or concerns known to staff

Academy Committee

The academy committee is responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible
- Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons

7. In the event a staff member self-isolates, with no impact on class bubble

In the event that a staff member is self-isolating but their associated bubble is not self-isolating, then the following should take place:

- Any pre-arranged or necessary meetings with parents/carers or outside agencies will continue to take place remotely. Staff members will conduct these from home. Staff members should discuss with SLT any difficulties with this, as soon as they know they will not be present as originally planned
- Teachers will live stream one session (no more than 20 minutes) a day and set work on Purple Mash or just work depending on health of a member of staff.
- If the activity set comprises of worksheets or similar, these will need to be emailed to the T.A. for printing and distributing in school. Where there is not a T.A. present, please liaise with colleagues (including admin team and SLT) to work an alternative
- Once a calendar week, in line with iPad availability, teaching staff to set the activity on Purple Mash and provide feedback during the session (via Purple Mash)
- Sessions delivered could be the same lesson each day, or a variety. They could include any lesson normally delivered in school (R.E., English, Maths, Collective Worship, Reading etc.)
- Teaching Assistants will pre-record (either voice or video) a reading of an appropriate book and comprehension questions for the children to answer.

<u>When recording or live streaming a lesson</u>
As above, when recording or live-streaming a lesson, staff must take due care and attention to avoid any loud, disruptive or inappropriate background noise or objects.
If staff do not feel they can achieve the above, they must discuss this with SLT.

8.Links with other policies and development plans

This policy is linked to our:

- Safeguarding
- Behaviour policy
- Child protection policy
- Data protection policy
- Online safety acceptable use policy
- E-safety policy

We will aim to provide this provision in the event of a whole- school closure. However, each case will be assessed on an individual basis and school reserve the right to adapt this plan when necessary.

Appendix 1

Option 1: Model timetable for whole-bubble closure *(will be adapted by teachers to reflect in-school timetable)*

Time	Activity
9:00am	Welcome session- good morning and morning prayer- see Purple Mash
9:15am	Reading/Writing/Maths – set on Purple Mash
10:15am	Break
10:30am	Reading/Writing/Maths – set on Purple Mash
11:30am	Handwriting/Spellings/
12:00pm	Lunch (don't forget to say your prayers) followed by free time
1:00pm	R.E./Topic/Science/Physical Activity – Set on Purple Mash
2:00pm	R.E./Topic/Science/Physical Activity/ Collective Worship – Set on Purple Mash
3:00pm	End of day prayer and dismissal

Option 1:Model timetable for whole-bubble closure - Reception *(will be adapted by teachers to reflect in-school timetable)*

Time	Activity
9:00am	Welcome - good morning, morning prayer, story and/or song time
9:20am	Maths (including play-based activity ideas)
10:15am	Snack and Break
10:40am	Phonics
11.00am	Handwriting/Fine Motor Skills
11:10am	Play Based Learning Activities
12:00pm	Lunch (don't forget to say your prayers) followed by free time
1:00pm	R.E./Topic/Physical Activity
1.45pm	Break
2:00pm	Play Based Learning Activities
2.40pm	Collective Worship
3:00pm	End of day prayer

Home Learning Timetable Option 2:

	Group A
9.00 – 9.30	Online Teaching
9.30 – 10.00	Follow Up Activity
10.00 – 10.30	Class Activity
10.30 – 11.00	Break
11.00 – 12.00	Home Learning Lesson
12.00 – 1.00	Lunch
1.00 – 1.30	Online Teaching
1.30 – 2.00	Follow Up Activity
2.00 – 2.30	Class Activity
2.30 – 3.00	Alternate Activities
3.00 – 3.15	Reading

	Group B
9.05 – 9.35	Class Activity
9.35 – 10.05	Online Teaching
10.05 – 10.35	Follow Up Activity
10.35 – 11.05	Break
11.05 – 12.05	Home Learning Lesson
12.05 – 1.05	Lunch
1.05 – 1.35	Class Activity
1.35 – 2.05	Online Teaching
2.05 – 2.35	Follow Up Activity
2.35 – 3.05	Alternate Activities
3.05 – 3.20	Reading

Appendix 2

Model timetable for event where a small number of pupils are self-isolating, but able to access school work.

Time	Activity
8:00am	Wake up, have breakfast, get dressed, say the morning prayer
9:00am	Maths activity from Purple Mash
10:00am	Short brain break – any activity that takes you away from school work
10:05am	English activity from Purple Mash
11:15am	Handwriting/Spelling/Collective Worship/Reading
12:00pm	Lunch (don't forget to say your prayers) followed by free time
1:00pm	Topic, Science or RE activity from Purple Mash
2:00pm	Short brain break – any activity that takes you away from school work
2:05pm	Topic, Science or RE activity from Purple Mash
3:00pm	End of day prayer

Appendix 3

Code of Conduct for phone calls, video calls and recorded video

For Pupils

- I will only take part in 'live 'video calls/sessions if an adult at home knows that I am doing it.
- I will not reveal my passwords to anyone.
- I will be responsible for my behaviour and actions when using technology (Zoom, Purple Mash and Other interactive applications), this includes the resources I access and the language I use.
- I will make sure that all my communication with pupils, teachers or others using technology is responsible and sensible.
- I will not deliberately browse, download, upload or forward material that could be considered inappropriate. If I accidentally come across any such material I will report it immediately to my teacher or my parent/carer.
- I will not share resources or videos created by my teachers with anyone who is not a pupil or member of staff at St Ambrose Catholic Primary School
- I will not record or take photos of my classmates or teachers during a face-to-face session.
- I will not share any school content on social media platforms
- I understand that when using Teams and other applications provided by the school that my use can be monitored and logged and can be made available to my teachers.
- I will continue to follow the rules (where applicable to home learning) regarding my use of technology as outlined in the school's Pupil Acceptable User Agreement
- I understand that these rules are designed to help keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

Code of Conduct for phone calls, video calls and recorded video

For Staff

- To continue to follow Safeguarding procedures, including (but not limited to) continuing to look out for signs that a child may be at risk and reporting to DSLs.
- Staff must only use platforms agreed by the school to communicate with pupils, and it is the responsibility of the teachers to check content and comments.
- 1:1 video calls are strictly prohibited – On no occasion should staff make or take video calls with pupils.
- Wherever possible, another member of staff should be present/logged into live video calls
- Suitable clothing should be worn by all adult, in line with SNOMAC's Staff Professional Appearance Policy
- Language and behaviour must be professional and appropriate.
- Staff should ensure they are working from a suitable area at home, especially when using live video or recorded video
- Staff must ensure any background in videos (including background noise) is appropriate. This includes ensuring other household members are not included in any live lesson or video
- Staff should ensure there is always a meeting password and waiting room enabled for live video calling
- Staff will follow usual behaviour management techniques, used in school, to address any positive or concerning behaviour.
- Staff will contact parents/carers by email if pupils do not adhere to their Code of Conduct

Appendix 4

Pupil Acceptable Use Policy

Rules for Responsible Internet Use

Foundation/ KS1 Pupil Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

This is how we stay safe when we use ICT:

- I will ask a teacher or suitable adult if I want to use the computers, tablets, interactive whiteboards or other computing equipment.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child):

Signed (parent):

Date

STAFF ACCEPTABLE USE POLICY

Who Does It Apply To?

This policy applies to all staff. This Acceptable Use Policy is intended to provide a framework for the use of St Ambrose Catholic Primary School. It applies to all computing, telecommunication, and networking facilities.

Basis for Policy

IT systems are critical for the day to day functions of governance, management, administration, parental links and involvement, teaching and learning. Computerised information technology resources available for Academy staff, parents and students will continue to grow and develop.
The protection of these resources is therefore of vital importance.

It is of equal importance that the community of users are themselves protected as far as is reasonably practicable from any potential harm that may result from unacceptable, uninformed and inappropriate use.

In order to facilitate the above every potential member of the community of users has to:

1. a) Understand what is and is not acceptable action and behaviour (acceptable use).
2. b) All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
3. c) Agree to abide by and follow ‘acceptable use’ through the signing of an agreement.
4. d) Understand and accept that sanctions may apply for breaches of acceptable use and that this could include suspension, dismissal, exclusion or criminal prosecution.

IT Equipment (Including Cabling)

1. Treat all equipment with care and respect so as to cause it no damage whatsoever.
2. Do not use any equipment that you believe to be damaged or unsafe.
3. Report immediately any damage to the equipment that you become aware of.
4. Do not dismantle any part of the equipment (including a mouse or other peripheral device).
5. Do not move any equipment.
6. Do not relocate any piece of equipment within the school unless you are authorised to do so.
7. Do not remove any part of the equipment from site unless you are authorised to do so.
8. If you are aware of anyone damaging, stealing or misusing equipment you must report it to a teacher or senior member of staff immediately.
9. Do not eat or drink whilst using IT equipment.
10. Staff should not connect any equipment or devices to the network without the prior approval of the Network Manager.

Software

1. No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the computer systems is put at risk if users do not take adequate precautions against malicious software.
2. Staff must not install, or attempt to install, programs of any type on a machine, or store programs on the computers without permission.
3. Staff must not deliberately damage, disable or otherwise harm the operation of software on computers.
4. Staff must not deliberately create, distribute or install agents designed to or are likely to hamper, disable, disrupt or damage any part of the IT infrastructure, equipment or software e.g. viruses, worms or bombs etc.
5. The distribution or storage by any means of pirated software is prohibited.

Mobile Devices

1. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following classifications;
    - Laptop/notebook/netbook/tablet computers
    - Memory Sticks/USB Storage Media
    - PDAs
    - Any mobile device (including phones) capable of storing data
2. The school is committed to aiding staff to make use of new technology and as such staff are able to access the wireless network with their personal devices during the school day.
3. It is imperative that any mobile device be utilized appropriately and responsibly. The use of private equipment during lessons is forbidden unless there is a positive educational value.
4. It is the user’s responsibility to ensure that no viruses are enabled through negligence. Any mobile device brought onto school premises should be virus free and checked on a regular basis.
5. It is the responsibility of any user who uses a mobile device to ensure the security of stored data. Data must not be downloaded and copied from the network or attached machines unless you have lawful and appropriate authority to do so.
6. All mobile devices must be password protected, and all data stored on the device must be encrypted using strong encryption.
7. Staff using a personal smartphone to receive/send school email must ensure that the phone is password/PIN/fingerprint/facial recognition protected.
8. Staff using a personal smartphone to access SIMS data must ensure that the phone is password/PIN/fingerprint/facial recognition protected.
9. The school reserves the right to refuse the ability to connect mobile devices to the school network infrastructure, if it feels such equipment is being used in a way that puts the school systems and data at risk.
10. The school accepts no responsibility for any loss, damage, or theft of devices or documents on such devices and it is brought into school at the user's own risk.
11. Any sensitive data to be transported must be via an encrypted device (see below).

Hardware Encrypted USB

All staff are required to store and transport sensitive data via a secure method. For this reason, staff are provided with a hardware encrypted USB device that should be used for all secure sensitive data being transported. Please read the following;

Sensitive data is defined as information that is protected against unwarranted disclosure. Protection of sensitive data may be required for legal or ethical reasons, pertaining to personal privacy or for proprietary considerations.

- You should not store any sensitive or personal information (including school related photographs) about staff or students on any other portable storage system (such as a non- secure USB memory stick, portable hard drive, or laptop computer) unless that storage system is encrypted and approved for such use by the school. No such data may in any event be stored on any privately owned device.
- You should not divulge your encrypted USB password to anyone else.

- On no account should you attempt to dismantle the encrypted USB. This may expose you or others to risk of physical harm and may invalidate any warranty. If you do this, you will be held liable for any subsequent repair or replacement costs.
- The equipment is on loan to you for professional use only i.e. for work related to your teaching/management role within the school and is subject to review.
- If you cease to be a member of staff, you must return the device prior to your departure. If you fail to do so you will be sent a bill for the full cost of an equivalent replacement.
- Encrypted USB devices that are no longer required, or have become damaged, must be returned to the IT Support Department for secure disposal.

Passwords and Security

All individually allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they are allocated.

Data security is of paramount importance, ensuring the privacy and protection of personal data. The user is personally responsible and accountable for all activities carried out under their username.

1. Staff must not disclose their password to others, or use passwords intended for the use of others. The password associated with a particular personal username must not be divulged to any other person, other than to designated members of IT staff for the purposes of system support.
2. Passwords used must adhere to current password policy and practice and should be changed immediately from any default password supplied. Passwords for any computer system/application should not be easy to guess and should not be kept on post it notes stuck to PC equipment.
3. Access to the School Information Management System (SIMS) is provided on the understanding that it contains a vast amount of personal data on both staff and students alike and should not be left open to abuse. The unauthorized access of data, particularly SIMS related data is taken extremely seriously. You should ensure your computer is not accessible by anyone other than yourself when logged into SIMS.
4. Under no circumstances should any user disguise, attempt to disguise or mask their identity.

5. All users are expected to respect and not attempt to bypass security in place on the computer systems.
6. Attempts to access or use any username, e-mail address, which is not authorised to the user, are prohibited.
7. Users must not attempt to alter the settings of computers unless they are authorised to do so.
8. All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
9. All users should understand that network activity and online communications are monitored, including any personal and private communications made via school devices.
10. When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
11. You should not store any sensitive or personal information about staff or students on any other portable storage system (such as a non-secure USB memory stick, portable hard drive, or laptop computer) unless that storage system is encrypted and approved for such use by the school. No such data may in any event be stored on any privately-owned device.
12. Remote access to school resources are provided to staff via various solutions. Staff should take all necessary precautions to ensure that no unauthorised persons can gain access. Remote sessions with the school must be closed appropriately at the end of each session
13. Files containing sensitive information must be encrypted and/or password protected.
14. You must make your own backup of data kept on any storage system other than the school network; this includes any data on the local drive of your school provided laptop.

Commercial, Business, Buying and Selling

1. All work produced using school equipment/ resources are the property of the school.
2. Staff must not use the network/equipment for personal business interests unrelated to school business.
3. Staff must utilise access to the Internet responsibly.

Internet Guidelines

The school subscribes to an accredited Broadband service as its ISP (Internet Service Provider) which provides an effective and safe e-learning environment including Internet access and e-mail service.

To safeguard against risks and unacceptable materials and activities these services include filtering and content control, firewall and virus protection and monitoring systems.

1. The school reserves the right to monitor internet usage.
2. Staff must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
3. Staff must report accidental accessing of unsuitable sites to the IT Support team.
4. Staff are expected to respect the work and ownership rights of people outside the school as well as other students and staff. This includes abiding by copyright laws; downloading, distribution,

or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder.

5. The copying of other people's web site material without the express permission of the copyright holder is prohibited.
6. Members of school staff are expected to take responsibility for the actions of any guests or visitors who they allow to use the school Internet facilities. Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.

Use of Social Networking Websites and Online Forums

Staff must take care when using social networking websites such as Facebook or Twitter even when such use occurs in their own time using their own computer. Social networking sites invite users to participate in informal ways that can leave you open to abuse;

- You must not allow any student to access personal information you post on a social networking site even for school-related purposes.
- You must avoid contacting any student privately via a social networking website. You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff wishing to make use of Social Networking Sites to support their teaching must be aware of the above guidelines, as well as following this procedure:

- Discuss and agree the plan with the SLG members responsible for Safeguarding and e- Learning.
- Set up ID’s which are for school use only, registered using school e-mail addresses, having no overlap or link to any personal ID’s.
- Lodge a copy of the full login details with the Network Manager, who may monitor content at any time (to report any inappropriate findings back to SLG).
- Treat behaviour and discipline as they would any lesson or other school activity.
- You should ensure that any social networking group you create for students to utilise take place within clear professional boundaries is transparent and open to scrutiny.

Digital Reputation

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Your digital reputation is defined by your behaviours in the online environment and by the content that you post about yourself and others. Think before you post, send or blog.
- Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school’s reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a student, that could potentially be used to embarrass, harass, or defame the subject.
- If you have a personal social networking profile, you should ensure this is set to private, checking occasionally to make sure the settings haven’t changed.

- You must at all times comply with DFE Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings (March 2009 and any revisions issued). Particular attention should be paid to contact with students and former students in the context of social networks.

Cloud

There are now many options for storing data in the cloud. Any staff member wishing to store work related data in this fashion must ensure that any potentially sensitive data is both password protected and encrypted.

Sensitive Information relates to personal information which may be subject to further regulations under the Data Protection Act 2018. Data security is of paramount importance, ensuring the privacy and protection of personal data.

Privacy

The school has legal duties in respect of the safeguarding and protection of students. Staff are required by school policy to divulge the contents of any communication that they become aware of, to the Head Teacher or other nominated Child Protection Officer, if, in their opinion, the content gives rise to any potential concern for a students' wellbeing.

These communications may in turn be shared with other statutory bodies charged with child protection as required by law.

After a member of staff leaves, any data associated with the account will be considered to be the property of the school and the account will be closed. Data will be archived for a period in accordance with normal backup procedures prior to being deleted from the records held.

Legal

Any software and / or hard copy of data or information which is not generated by the user personally and which may become available through the use of school systems shall not be copied or used without permission of the school or the copyright owner. Such permission must be obtained in writing and in the event of the copyright owner not being the school; the school must be supplied with a copy of any permission obtained. It is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them.

In the case of private work and other personal use of computing facilities, the school will not accept any liability for loss, damage, injury or expense that may result.

Email Cautionary Note

Staff are reminded that in legal terms, email on an employer's system is not 'private' and, in certain circumstances, employers can access and read employees emails.

The monitoring of email activity, especially in environments where child protection is an issue, is considered to be a matter a good practice.

Emails are routed through the County Council system and are therefore scanned for inappropriate language (including profanities) and content. Not only will the user be informed of any transgression but the school's senior management will also be alerted and sent a copy.

Confidential files should not be sent via email and other more secure methods should be sought. At the very least files containing sensitive data should be encrypted and password protected when sent via email.

Staff communication with students should only be conducted via their school email account and never from a personal/home account.

Policy

The use of the e-mail system and the Internet within the school is encouraged as its appropriate use facilitates communication and improves efficiency. Used correctly, it is a facility that is of assistance to many employees. Inappropriate use however causes many problems ranging from minor distractions to legal claims against the school. This policy sets out the governors' view on the correct use of the e-mail system and explains how this can be achieved as well as the governors' response to inappropriate use.

Authorised Use

The e-mail system and the Internet are available for communication on matters directly concerned with school business. Employees using the e-mail system should give particular attention to the following points:

1. The standard of presentation. The style and content of an e-mail message must be consistent with the standards that the school expects from written communications.
2. The extent of circulation. E-mail messages should only be sent to those employees for whom they are particularly relevant. It is not good practice to forward emails to a third party as indiscretions can often inadvertently result.
3. The appropriateness of the e-mail. Where and when not to use E-mail is a matter of individual judgement but care should be. CARE !! Copy missing??????
4. Ensure that it is not used as a substitute for face-to-face communication when such communication is more appropriate. "Flame-mails" (e-mails that are abusive) can be a source of stress and damage work relationships. Hasty messages sent without proper consideration can cause unnecessary misunderstandings.
5. The visibility of e-mail. If the message is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The school will be liable for any defamatory information circulated either within or to external users of the system.
6. E-mail contracts. Offers or contracts transmitted via e-mail are as legally binding on the school as those sent on paper.

Unauthorised Use

The school will not tolerate the use of the system for any of the following:

1. Any message that could constitute bullying or harassment (e.g. on the grounds of sex, race or disability).
2. Personal use in school time e.g. social invitations, personal messages, jokes, cartoons or chain letters.
3. On-line gambling.
4. Accessing pornography or inappropriate images.
5. Downloading or distributing copyright information and / or any software available to the user to others.
6. Posting confidential information about other employees, the school, students and their contacts or its suppliers.
7. Extremist or radicalised behaviour.

Implementation of the Policy

1. The Network Manager is the manager of the system and will be available to give advice on all aspects of the policy.
2. Regular monitoring and recording of e-mail messages will be carried out on a random basis by the Network Manager. Hard copies of improper e-mail messages may be used as evidence in disciplinary proceedings.
3. All e-mail users will have a unique identity and password. The password is to be changed regularly and is confidential to the user. Access to the e-mail system using another employee’s ID and password without prior authorisation is likely to result in disciplinary action including summary dismissal.
4. Users must ensure that critical information is not stored solely within the e-mail system. If necessary, documents must be password protected.
5. Users are required to be familiar with the requirements of the Data Protection Act 1998 and to ensure that they operate in accordance with the requirements of the Act.
6. Employees who feel that they have cause for complaint as a result of e-mail communications should raise the matter initially with their immediate manager or the Network Manager. If necessary, the complaint can be dealt with under the grievance procedure.

It should be noted that individuals may be held responsible for the retention of attachment material that they have received. Similarly, opening an attachment, received via unsolicited ‘phishing’ e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken.

Sanctions – Failure to comply with these rules will result in one or more of the following.

If the law is broken, then 5 may apply in certain circumstances. Such action may be invoked by external agencies or organisations.

1. An oral or written warning.
2. Restricted use of equipment (including the confiscation of loaned equipment such as a laptop).
3. A ban temporary or permanent from access to and the use of the school email system or entire network.

4. Disciplinary action which may in certain circumstances include dismissal.
5. Criminal prosecution.

Additional Information

Responsibility of a school provided laptop rests with the designated member of staff. Staff should ensure they have absolute control of a laptop allocated to their use. Persons not employed by the school including family members must not be allowed to use the laptop in any circumstances.

Loss of identifiable data (particularly sensitive data) is regarded as a serious incident and any such occurrence should immediately be reported to the St Nicholas Owen Chief Finance and Operations Officer.

Staff should also have read the St Ambrose Catholic Primary School E-Safety Policy.

Staff members should also read and be aware of guidance notes provided by Worcestershire County Council in the Managing Allegations against Adults Who Work with Schools and are in Educational Settings in Worcestershire document, number: 33A (September 2009). Sections of note in association with this Acceptable Use Policy are;

- Social Contact.
- Communications with Children Using Technology.
- Inappropriate Images and Internet Usage.

Any suspected breach of this Acceptable Use Policy should be reported to the Network Manager. The responsible senior member will then take the appropriate action. If any infringements are auto detected, IT support staff may alert the Network Manager and/or other senior staff member as appropriate. The school reserves the right to audit and/or suspend without notice any account pending any enquiry.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered, it is the intention of the senior leadership group to review this document regularly and any changes shall be communicated to all staff.

Staff should address questions concerning what is acceptable to either the Network Manager or St Nicholas Owen Chief Finance and Operations Officer.

Staff should also ensure they have read the St Ambrose Catholic Primary E-Safety Policy before using any school IT facilities.**ACCEPTABLE USE POLICY 2020**

MEMBER OF STAFF AGREEMENT

I understand the above and agree to use the school IT facilities in a responsible manner and in accordance with the Saint Ambrose School Acceptable Use Policy 2020.

Name: ....

Signed: ....

Date: ....